Amazon Simple Storage Service. S3.

S3 stores data objects in buckets.

An object consists of a file and optionally any metadata that describes that file.

A key is the unique identifier for an object within a bucket.

Storage capacity is virtually unlimited.

For each bucket, you can:

Control access to it (create, delete, and list objects in the bucket)

View access logs for it and its objects

Choose the geographical region where to store the bucket and its contents.

Bucket name must be a unique DNS-compliant name.

The name must be unique across all existing bucket names in Amazon S3.

After you create the bucket you cannot change the name.

The bucket name is visible in the URL that points to the objects that you’re going to put in your bucket.

By default, you can create up to 100 buckets in each of your AWS accounts.

You can’t change its Region after creation.

You can host static websites by configuring your bucket for website hosting.

Data Consistency Model.

read-after-write consistency for PUTS of new objects in your S3 bucket in all regions

eventual consistency for read-after-write HEAD or GET requests

eventual consistency for overwrite PUTS and DELETES in all regions

Storage Classes.

S3 - Standard

S3 - (IA) Infrequently Accessed

S3 - One Zone (IA) Infrequently Accessed

S3 - Intelligent Tiering (IA/Frequent Access Hybrid)

S3 - Glacier

S3 - Glacier Deep Archive

S3 API

REST – use standard HTTP requests to create, fetch, and delete buckets and objects. You can use S3 virtual hosting to address a bucket in a REST API call by using the HTTP Host header.

Subresources.

Location, Policy and Access Control List (ACL), CORS, Website, Logging, Event Notification, Versioning, Lifecycle, Cross-Region Replication, Tagging, Transfer Acceleration

Object.

Each object has data, a key and metadata.

Objects are private by default.

Object metadata cannot be changed once uploaded.

Metadata come in two kinds, system and user defined

You can upload and copy objects up to 5GB in size. Larger uploads must use the multi-part API.

10 Tags per object.

Lifecycle Management.

Transition actions. Move to another storage class.

Expiration actions. Delete expired objects.

Pricing.

Pay for storing objects.

Pay for requests.

Pay for retrieval in IA and Glacier Storage.

Pay for early deletes in IA and Glacier Storage.

Pay for storage management.

Pay for bandwidth except for internet traffic, same region EC2, CloudFront. Eg. Transfer Acceleration

Networking.

Hosted Style Access

Path Style Access

Customize URL with CNAMEs

Transfer Acceleration to edge locations

Transfer Acceleration cannot be disabled, only suspended.

Security.

Policies include

Resources for buckets and objects

Actions are a set of operations

Effect deals with allow or deny

Principal deals with the account, service or user and access

Resource Policies

Bucket Policies provide centralized access control based on conditions, they can add or deny permissions to objects

Access Control Lists grant permissions, cannot deny permissions, 100 granted permissions per ACL. S3 Log Delivery Group should be granted write permissions via ACL.

User Policies

AWS IAM

Versioning

Multiple versions

Disabled by default

Delete marker

Only suspend versioning

Only owner can permanently delete a bucket

Encryption. Server side and Client side

SSE-S3 Managed Keys

SSE-KMS Managed Keys

SSE-C

MFA Delete.

Monitoring.

Cloudwatch Alarms, watch a metric. Supports event history

Notifications.

Can publish object creation events, object removal events.

Supports destinations. SNS, SQS and Lambda

Cross Region Replication.

Asynchronous copying of objects across buckets in different regions.

Minimize latency.

Both buckets must have versioning.

If the owner of the source bucket does not own the object, they must have READ permissions on the object ACL.

What is replicated.

Objects created after you add a replication configuration.

Both unencrypted objects and objects encrypted using Amazon S3 managed keys (SSE-S3) or AWS KMS managed keys (SSE-KMS), although you must explicitly enable the option to replicate objects encrypted using KMS keys. The replicated copy of the object is encrypted using the same type of server-side encryption that was used for the source object.

Object metadata.

Only objects in the source bucket for which the bucket owner has permissions to read objects and access control lists.

Object ACL updates, unless you direct S3 to change the replica ownership when source and destination buckets aren’t owned by the same accounts.

Object tags.

What is not replicated

Objects that existed before you added the replication configuration to the bucket.

Objects created with server-side encryption using customer-provided (SSE-C) encryption keys.

Objects created with server-side encryption using AWS KMS–managed encryption (SSE-KMS) keys.

Objects in the source bucket that the bucket owner doesn’t have permissions for.

Updates to bucket-level subresources.

Actions performed by lifecycle configuration.

Objects in the source bucket that are replicas created by another cross-region replication. You can replicate objects from a source bucket to only one destination bucket.

Does not replicate deletes

Batch Operations is a new feature to manage billions of objects in S3.